(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 September 2003 (12.09.2003)

PCT

(10) International Publication Number
WO 03/075506 A1

(51) International Patent Classification[7]: H04L 9/06

(21) International Application Number: PCT/IB03/00946

(22) International Filing Date: 4 March 2003 (04.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02 02918 7 March 2002 (07.03.2002) FR

(71) Applicant *(for all designated States except US)*: **SCHLUMBERGER SYSTEMES** [FR/FR]; 50 AVENUE JEAN JAURES, F-92120 MONTROUGE (FR).

(71) Applicant *(for MC only)*: **SCHLUMBERGER MALCO INC** [US/US]; 9800 REISTERTOWN, OWING MILLS, MD 21117 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **GOUBIN, Louis** [FR/FR]; 4 rue Mizon, F-75015 PARIS (FR). **AKKAR, Mehdi-Laurent** [FR/FR]; 17 rue Lafouge, F-94250 GENTILLY (FR).

(74) Common Representative: **SCHLUMBERGER SYSTEMES**; C/O Patricia RENAULT, 36-38 Rue de la Princesse, BP 45, F-78431 LOUVECIENNES CEDEX (FR).

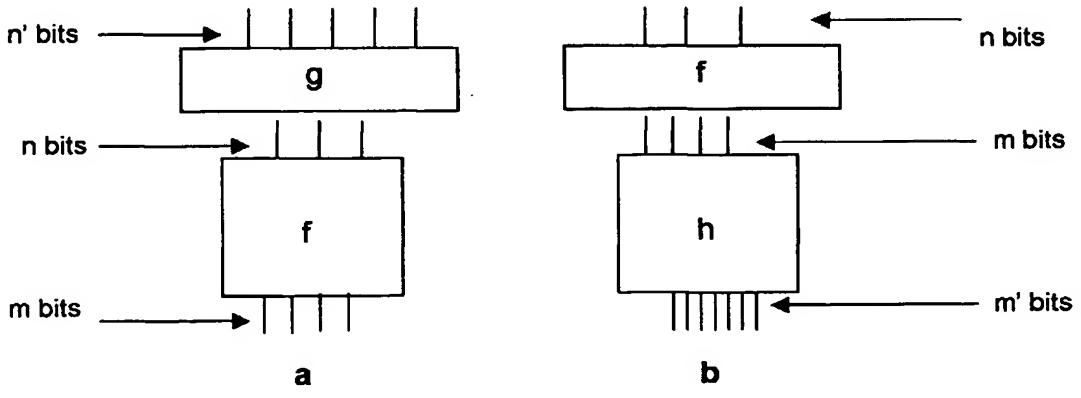
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD FOR MAKING SAFE AN ELECTRONIC CRYPTOGRAPHY ASSEMBLY WITH A SECRET KEY



(57) Abstract: An aim of this invention is to eliminate the risks of aggression "DPA of the n order" attacks, for all n values, of cryptography electronic assemblies or systems with a secret or private key. The process according to this invention concerns a securing process for an electronic system using a cryptographic calculation procedure using a secret key. The process consists of masking intermediate results in input or output of at least one critical function for the said procedure.

WO 03/075506 A1